OBLON ET AL (703) 413-3000
DOCKET #0039-7667-2RD SHEET 1 OF 28

FIG. 1

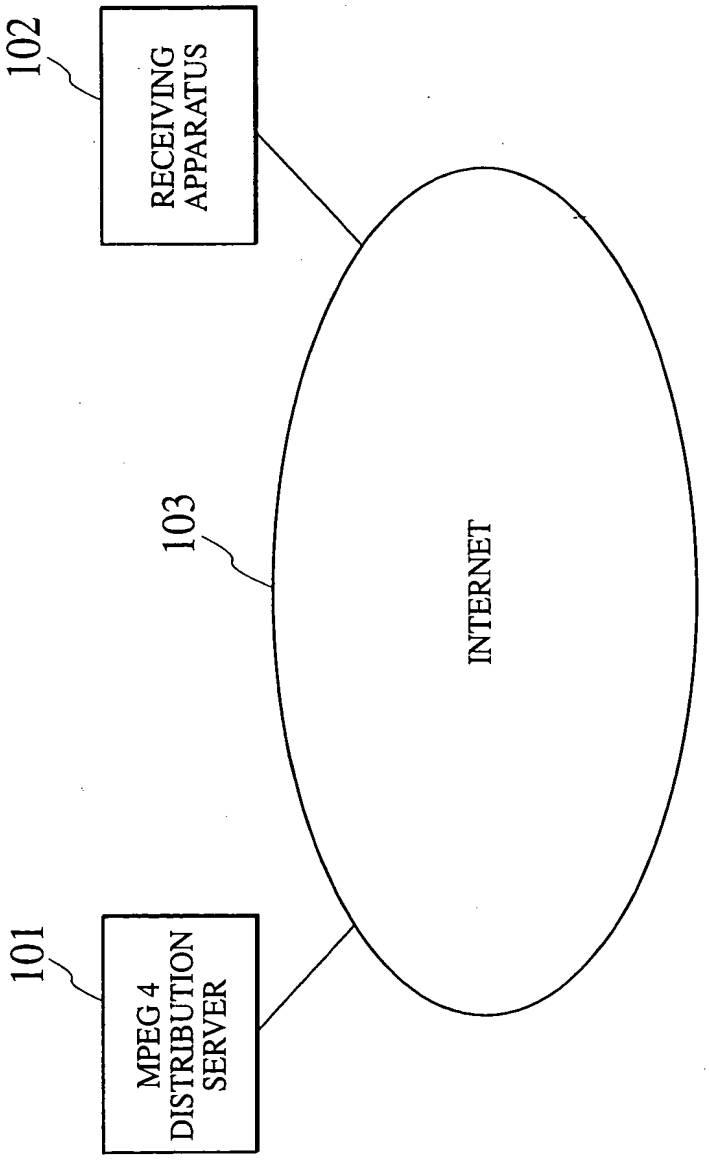
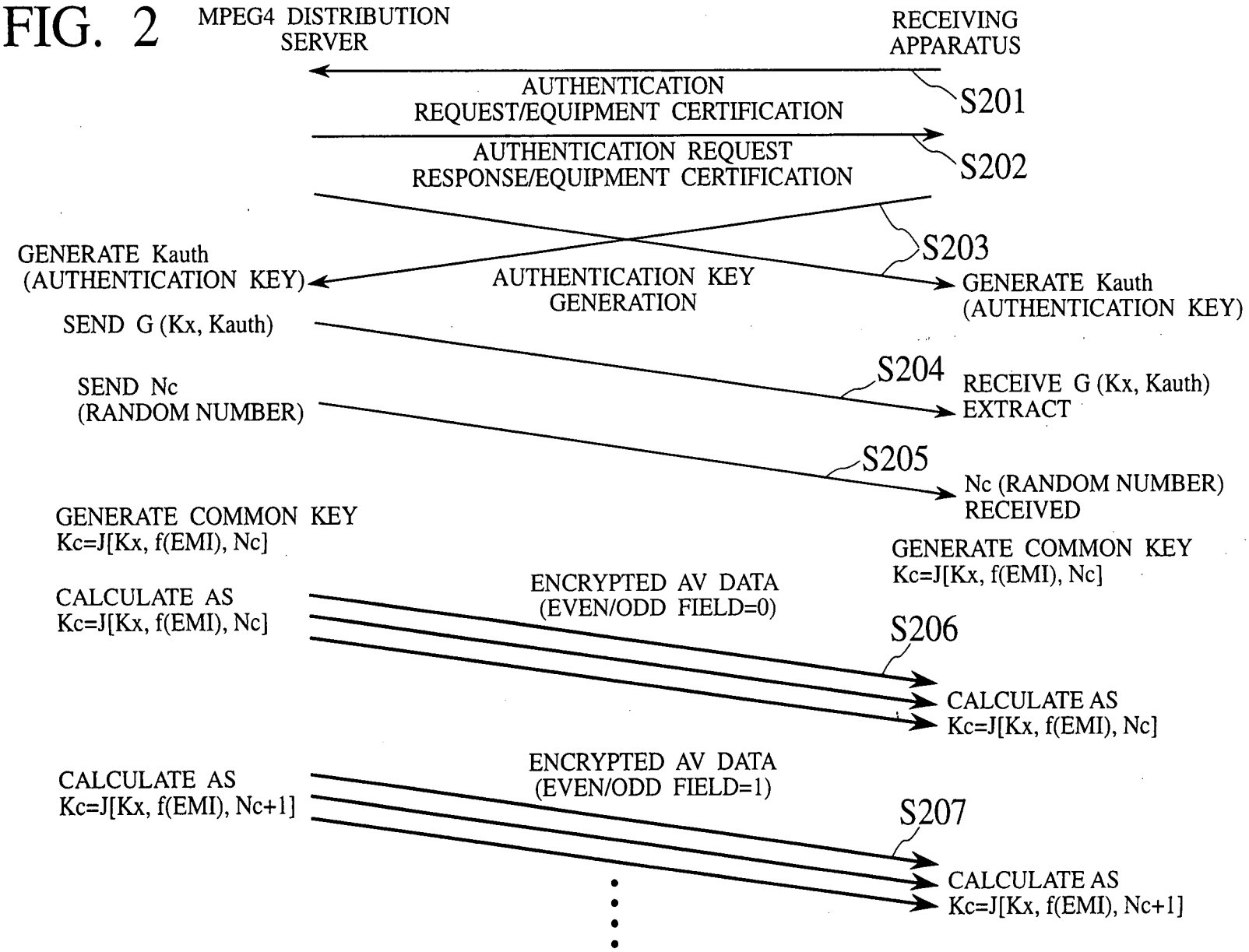


FIG. 2



OBLON ET AL (703) 413-3000
DOCKET #1039-766220 SHEET 2 OF 28

FIG. 3

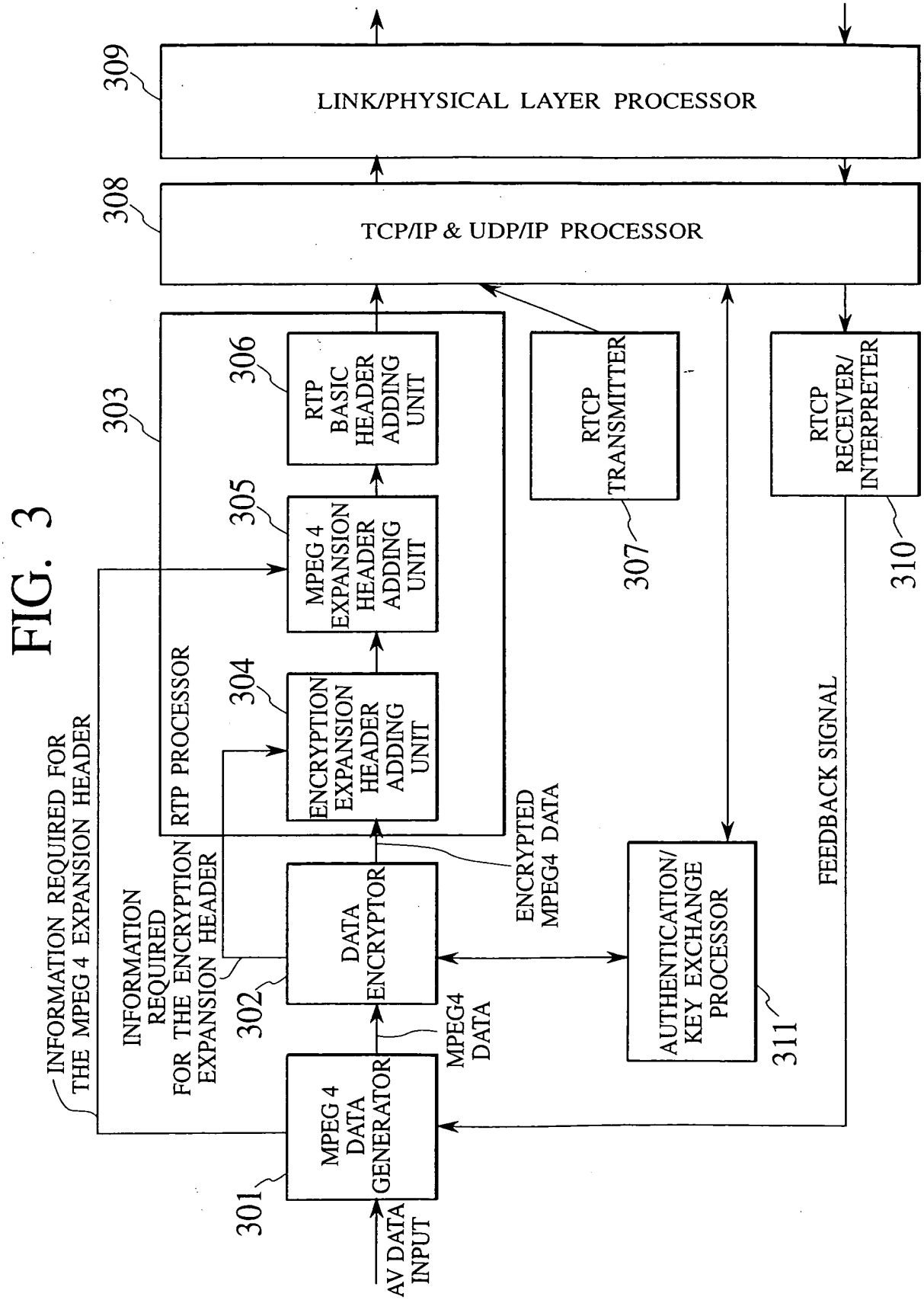

309
LINK/PHYSICAL LAYER PROCESSOR
308
TCP/IP & UDP/IP PROCESSOR
303
306
RTP BASIC HEADER ADDING UNIT
305
MPEG 4 EXPANSION HEADER ADDING UNIT
304
ENCRYPTION EXPANSION HEADER ADDING UNIT
RTP PROCESSOR
RTCP TRANSMITTER
307
RTCP RECEIVER/ INTERPRETER
310
INFORMATION REQUIRED FOR THE MPEG 4 EXPANSION HEADER
INFORMATION REQUIRED FOR THE ENCRYPTION EXPANSION HEADER
302
DATA ENCRYPTOR
ENCRYPTED MPEG4 DATA
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
311
FEEDBACK SIGNAL
MPEG4 DATA
301
MPEG 4 DATA GENERATOR
AV DATA INPUT

FIG. 4

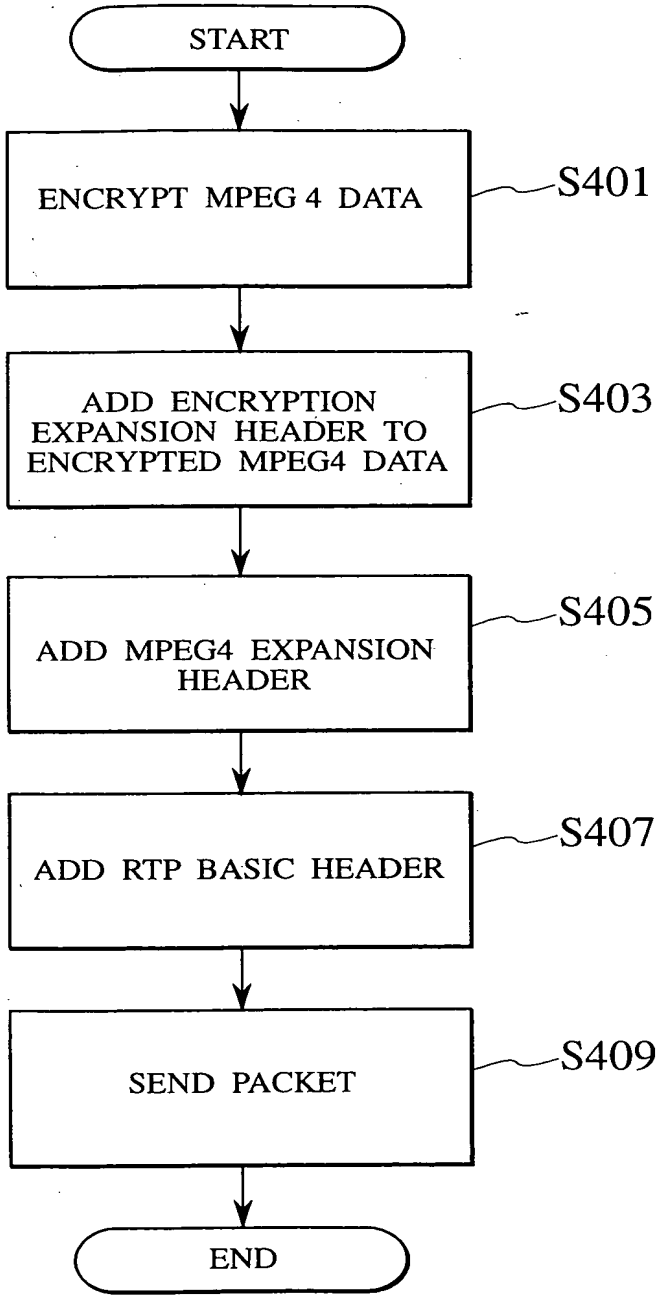

START
ENCRYPT MPEG 4 DATA
S401
ADD ENCRYPTION EXPANSION HEADER TO ENCRYPTED MPEG4 DATA
S403
ADD MPEG4 EXPANSION HEADER
S405
ADD RTP BASIC HEADER
S407
SEND PACKET
S409
END

FIG. 5

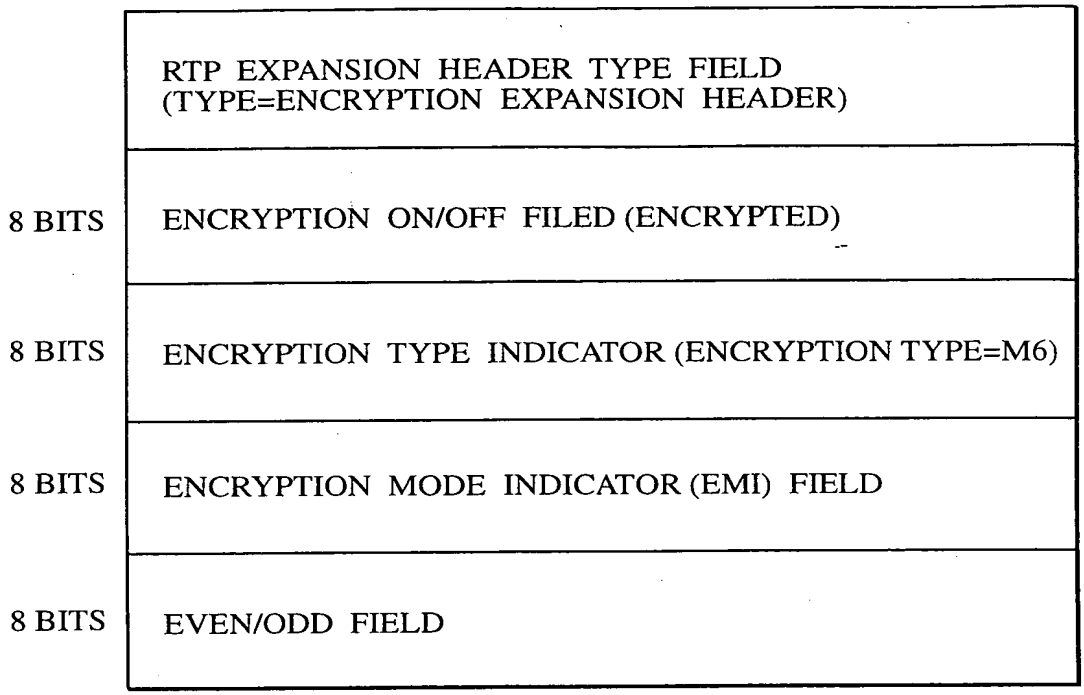

RTP EXPANSION HEADER TYPE FIELD (TYPE=ENCRYPTION EXPANSION HEADER)
8 BITS
ENCRYPTION ON/OFF FILED (ENCRYPTED)
8 BITS
ENCRYPTION TYPE INDICATOR (ENCRYPTION TYPE=M6)
8 BITS
ENCRYPTION MODE INDICATOR (EMI) FIELD
8 BITS
EVEN/ODD FIELD

FIG. 6

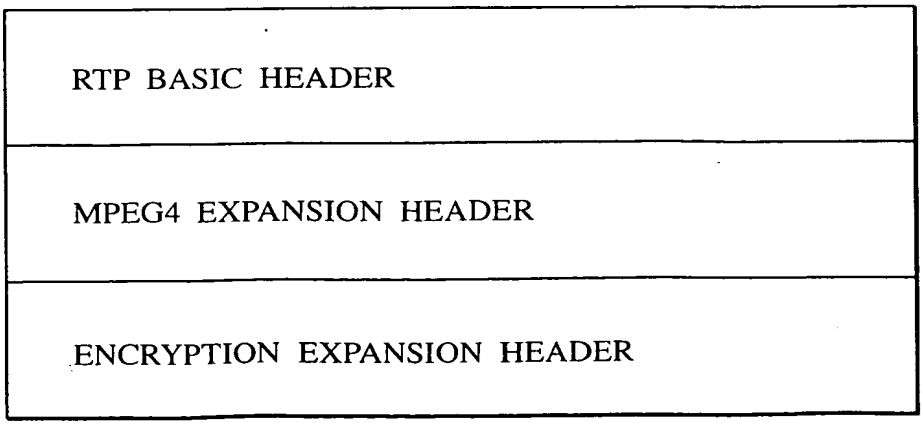

RTP BASIC HEADER
MPEG4 EXPANSION HEADER
ENCRYPTION EXPANSION HEADER

FIG. 7

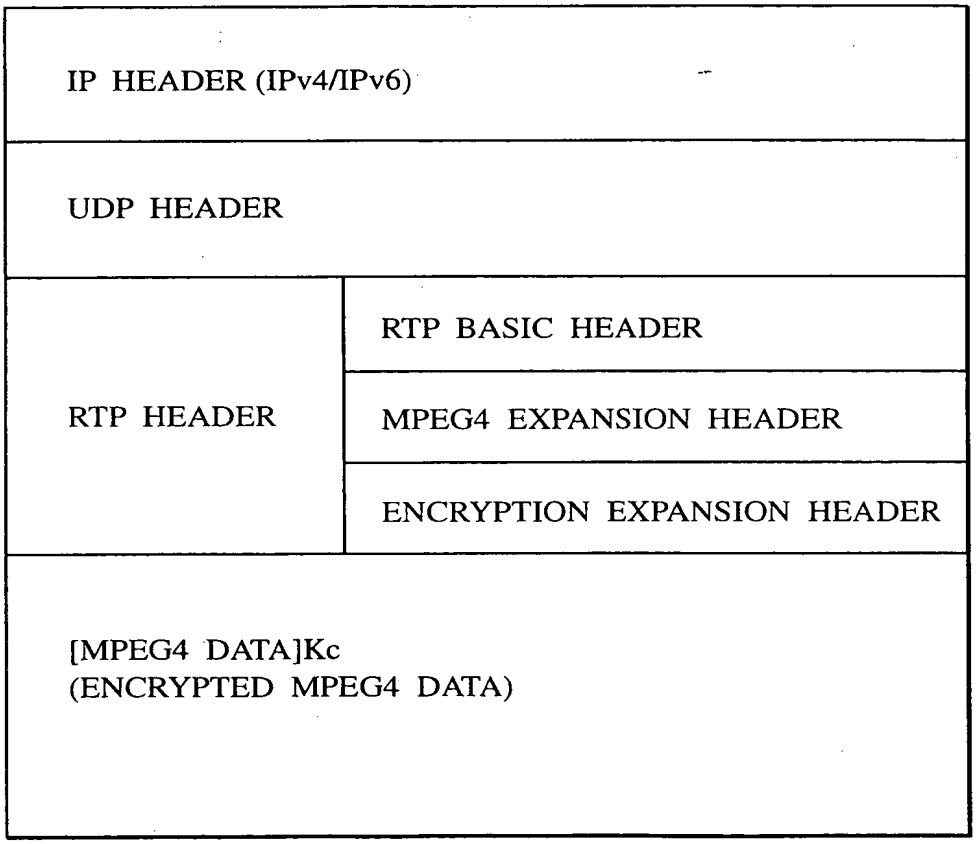

IP HEADER (IPv4/IPv6)
UDP HEADER
RTP HEADER
RTP BASIC HEADER
MPEG4 EXPANSION HEADER
ENCRYPTION EXPANSION HEADER
[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)

FIG. 8

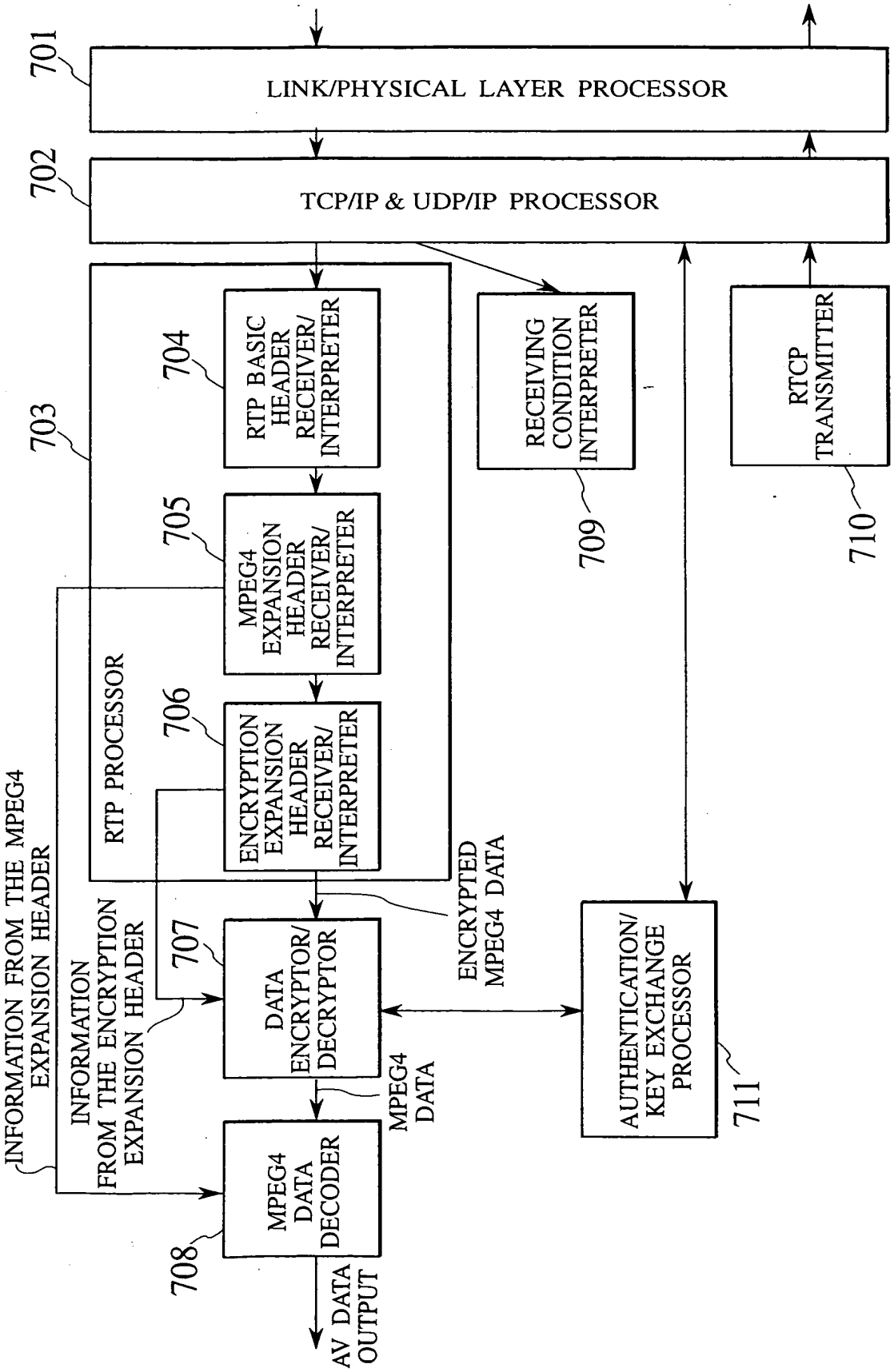

701
LINK/PHYSICAL LAYER PROCESSOR
702
TCP/IP & UDP/IP PROCESSOR
703
RTP PROCESSOR
704
RTP BASIC HEADER RECEIVER/ INTERPRETER
705
MPEG4 EXPANSION HEADER RECEIVER/ INTERPRETER
706
ENCRYPTION EXPANSION HEADER RECEIVER/ INTERPRETER
707
DATA ENCRYPTOR/ DECRYPTOR
708
MPEG4 DATA DECODER
709
RECEIVING CONDITION INTERPRETER
710
RTCP TRANSMITTER
711
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
INFORMATION FROM THE MPEG4 EXPANSION HEADER
INFORMATION FROM THE ENCRYPTION EXPANSION HEADER
ENCRYPTED MPEG4 DATA
MPEG4 DATA
AV DATA OUTPUT

FIG. 9

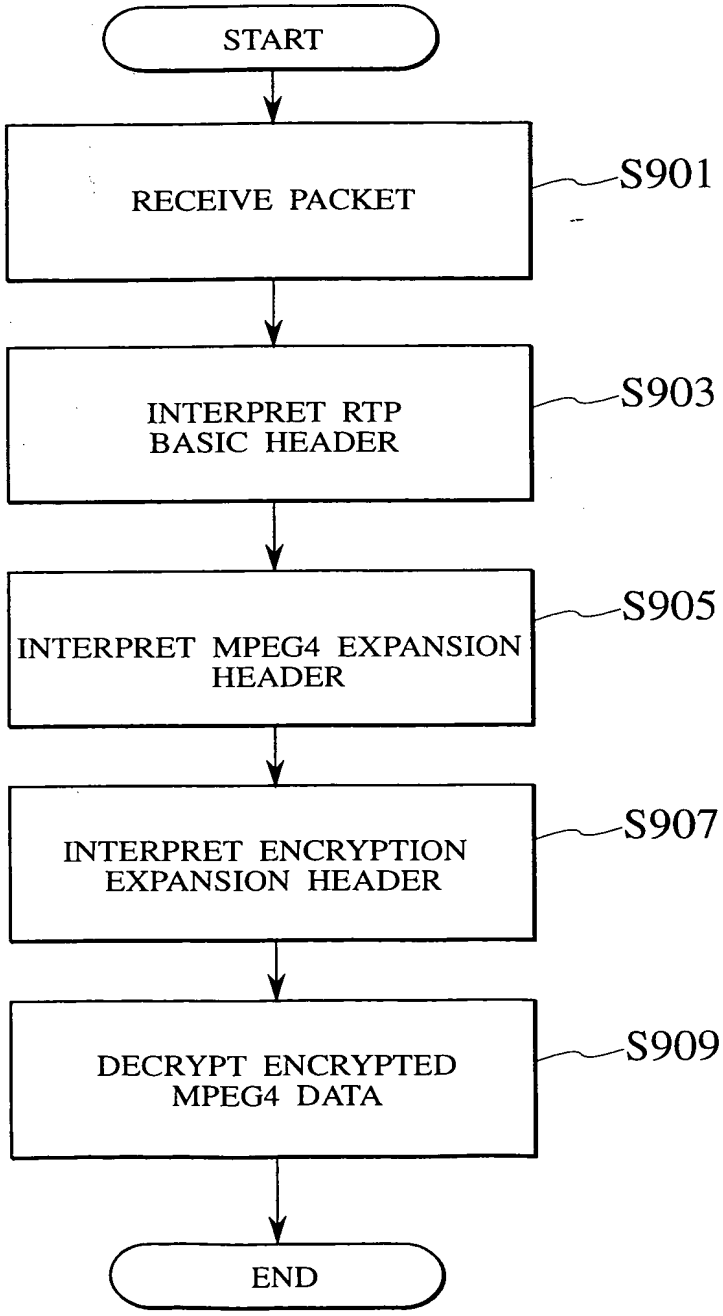

START
RECEIVE PACKET
S901
INTERPRET RTP BASIC HEADER
S903
INTERPRET MPEG4 EXPANSION HEADER
S905
INTERPRET ENCRYPTION EXPANSION HEADER
S907
DECRYPT ENCRYPTED MPEG4 DATA
S909
END

FIG. 10

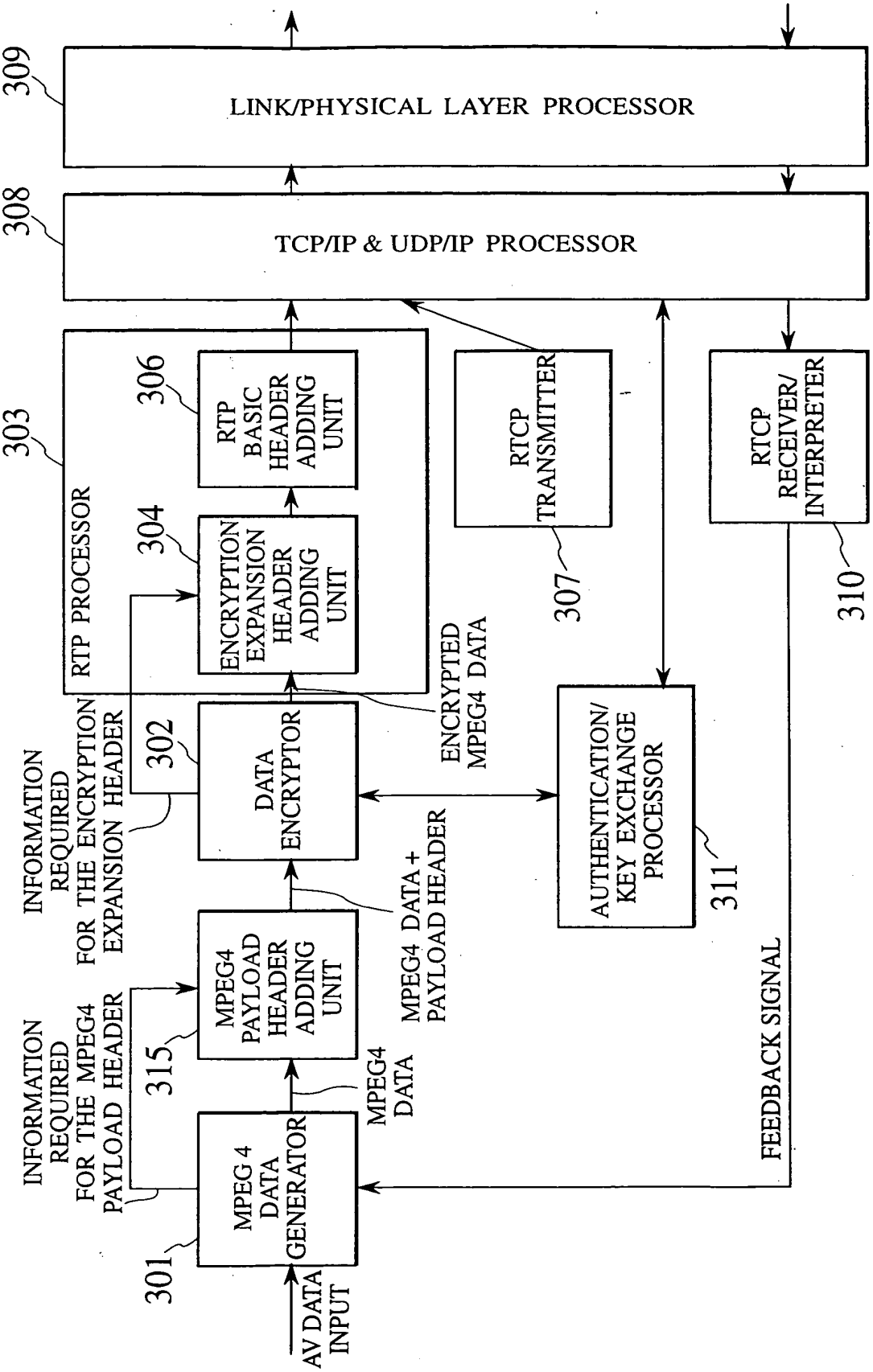

309
LINK/PHYSICAL LAYER PROCESSOR
308
TCP/IP & UDP/IP PROCESSOR
303
RTP PROCESSOR
306
RTP BASIC HEADER ADDING UNIT
304
ENCRYPTION EXPANSION HEADER ADDING UNIT
302
DATA ENCRYPTOR
315
MPEG4 PAYLOAD HEADER ADDING UNIT
301
MPEG 4 DATA GENERATOR
AV DATA INPUT
INFORMATION REQUIRED FOR THE ENCRYPTION EXPANSION HEADER
INFORMATION REQUIRED FOR THE MPEG4 PAYLOAD HEADER
MPEG4 DATA
MPEG4 DATA + PAYLOAD HEADER
ENCRYPTED MPEG4 DATA
RTCP TRANSMITTER
307
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
311
RTCP RECEIVER/ INTERPRETER
310
FEEDBACK SIGNAL

FIG. 11

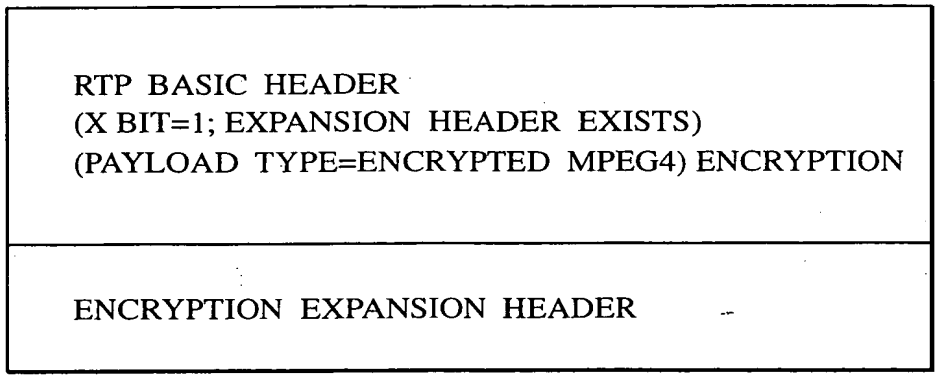
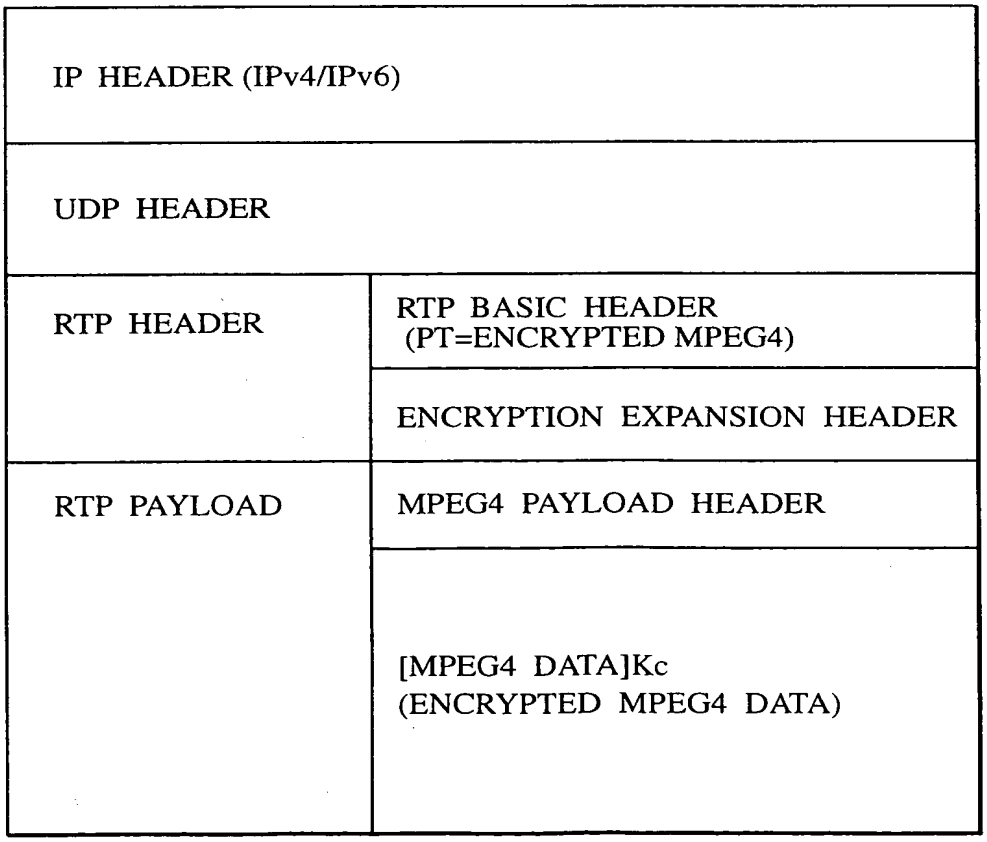


FIG. 12



6060260 "626250

FIG. 13

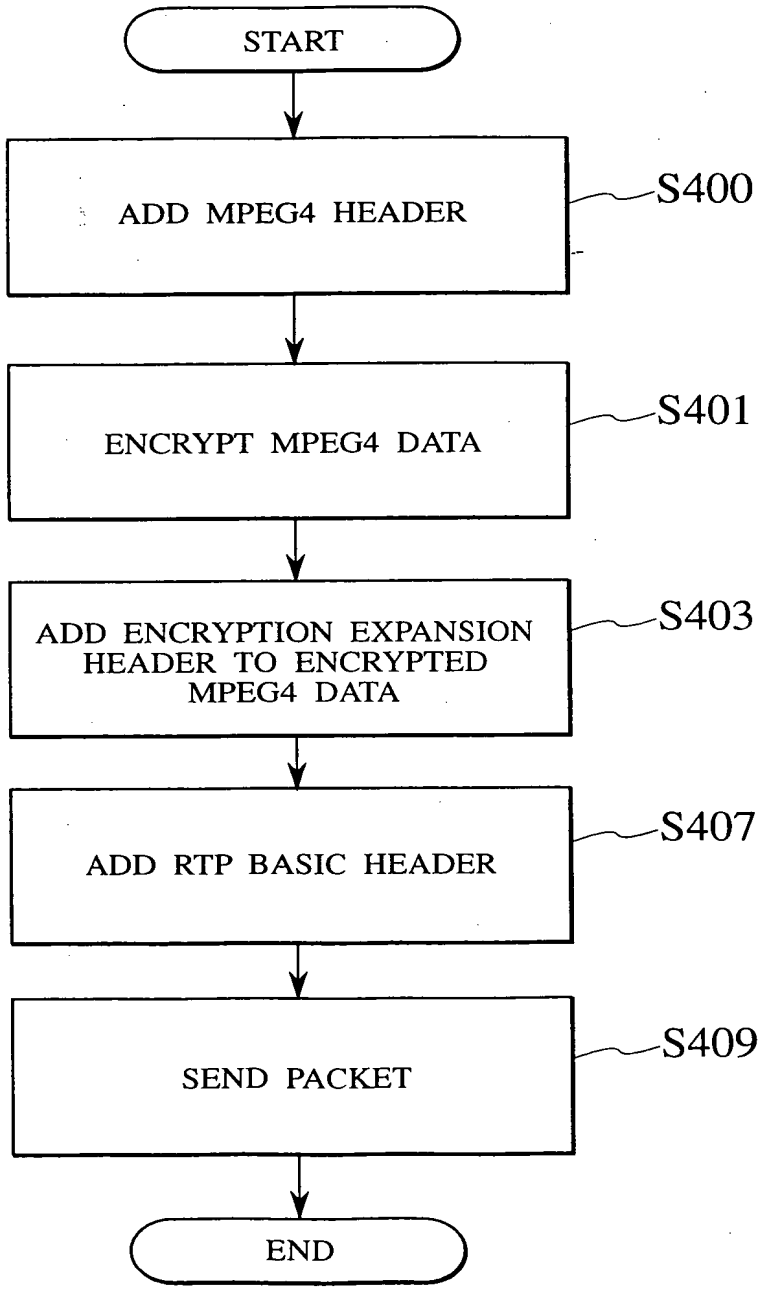

START
ADD MPEG4 HEADER
S400
ENCRYPT MPEG4 DATA
S401
ADD ENCRYPTION EXPANSION HEADER TO ENCRYPTED MPEG4 DATA
S403
ADD RTP BASIC HEADER
S407
SEND PACKET
S409
END

FIG. 14

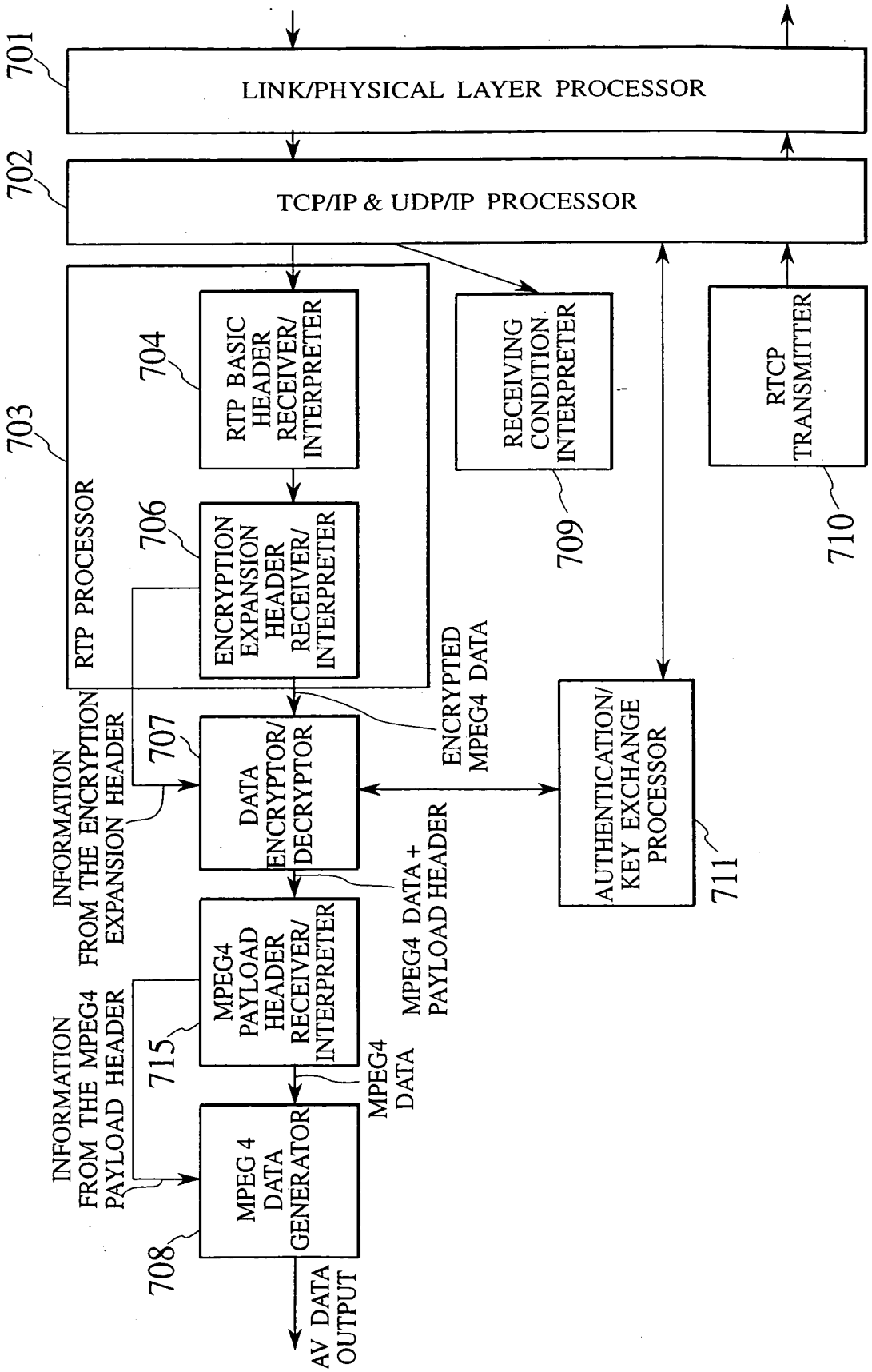

701
LINK/PHYSICAL LAYER PROCESSOR
702
TCP/IP & UDP/IP PROCESSOR
703
RTP PROCESSOR
704
RTP BASIC HEADER RECEIVER/ INTERPRETER
706
ENCRYPTION EXPANSION HEADER RECEIVER/ INTERPRETER
707
DATA ENCRYPTOR/ DECRYPTOR
715
MPEG4 PAYLOAD HEADER RECEIVER/ INTERPRETER
708
MPEG 4 DATA GENERATOR
AV DATA OUTPUT
INFORMATION FROM THE ENCRYPTION EXPANSION HEADER
INFORMATION FROM THE MPEG4 PAYLOAD HEADER
ENCRYPTED MPEG4 DATA
MPEG4 DATA + PAYLOAD HEADER
MPEG4 DATA
709
RECEIVING CONDITION INTERPRETER
710
RTCP TRANSMITTER
711
AUTHENTICATION/ KEY EXCHANGE PROCESSOR

FIG. 15

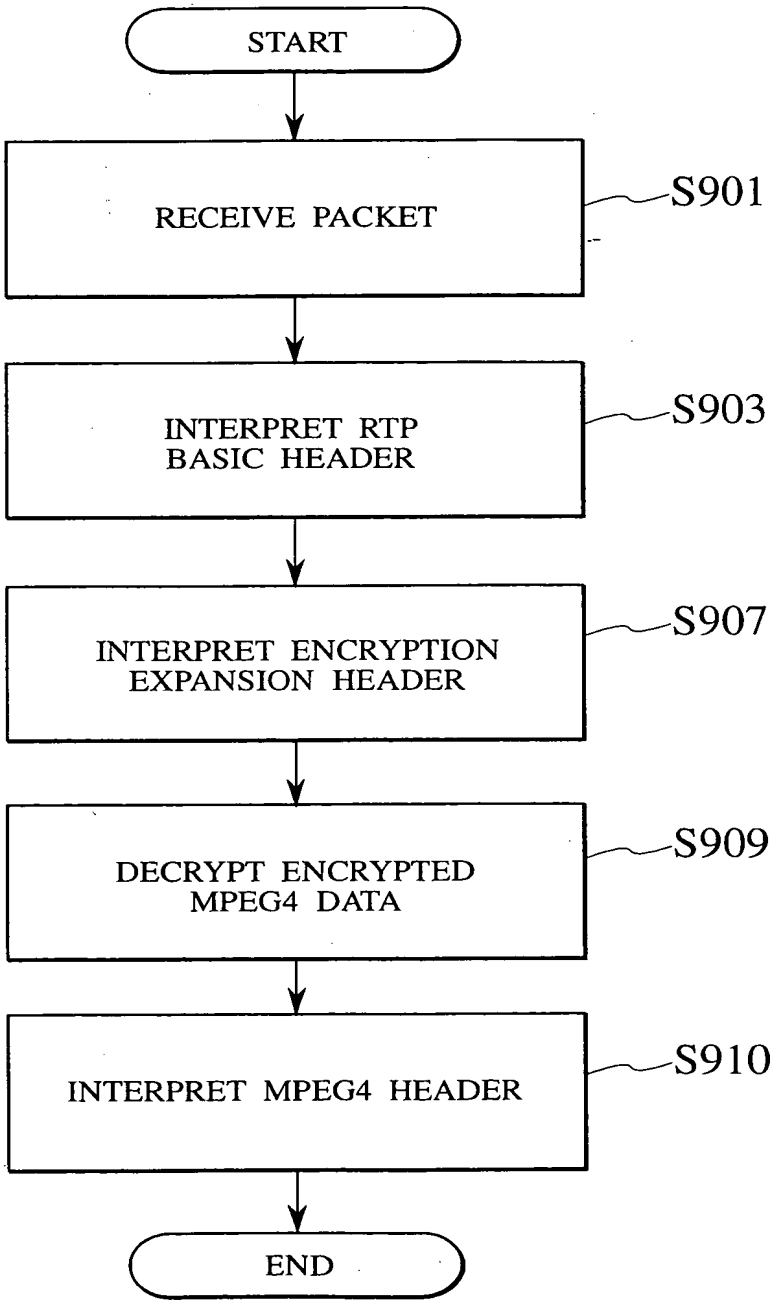

START
RECEIVE PACKET
S901
INTERPRET RTP BASIC HEADER
S903
INTERPRET ENCRYPTION EXPANSION HEADER
S907
DECRYPT ENCRYPTED MPEG4 DATA
S909
INTERPRET MPEG4 HEADER
S910
END

FIG. 16

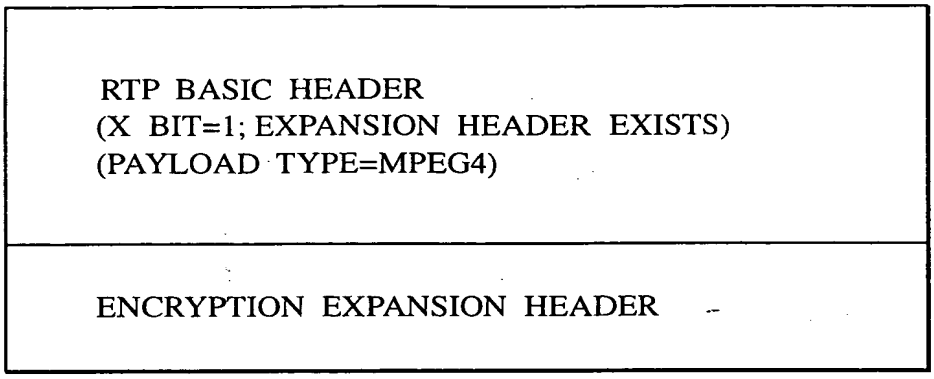
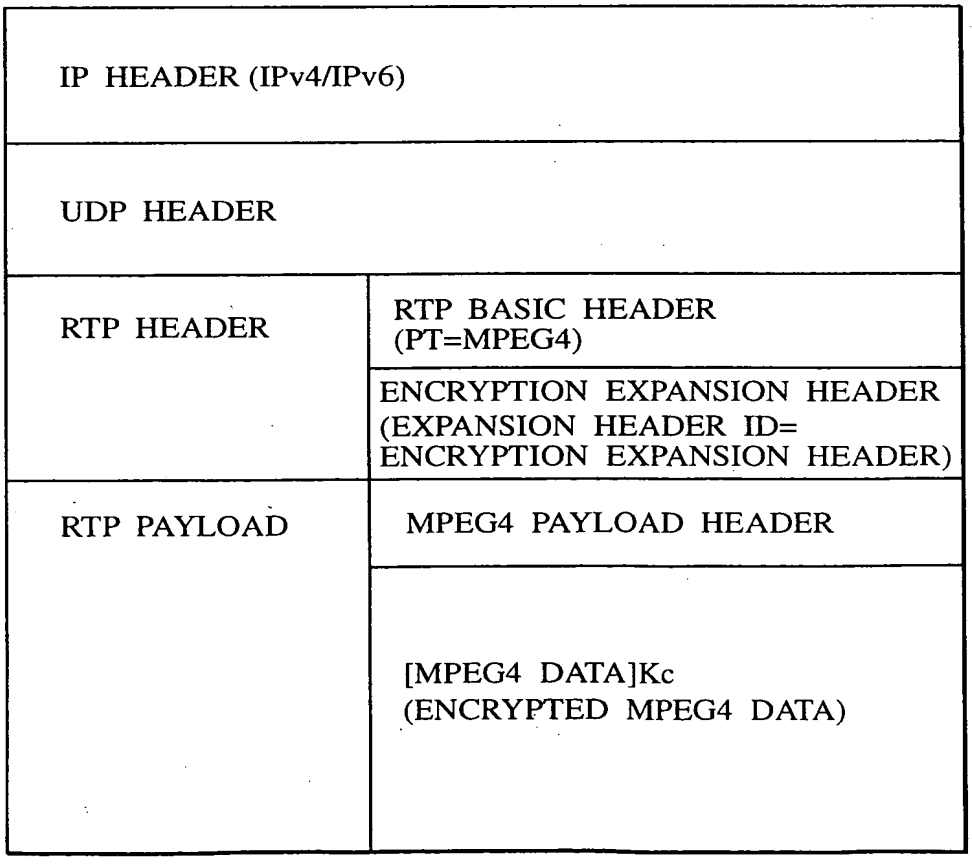

RTP BASIC HEADER
(X BIT=1; EXPANSION HEADER EXISTS)
(PAYLOAD TYPE=MPEG4)
ENCRYPTION EXPANSION HEADER

FIG. 17


IP HEADER (IPv4/IPv6)
UDP HEADER
RTP HEADER
RTP BASIC HEADER
(PT=MPEG4)
ENCRYPTION EXPANSION HEADER
(EXPANSION HEADER ID=
ENCRYPTION EXPANSION HEADER)
RTP PAYLOAD
MPEG4 PAYLOAD HEADER
[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)

OBLON ET AL (703) 413-3000
DOCKET #091-7667-200 SHEET 15 OF 28

FIG. 18

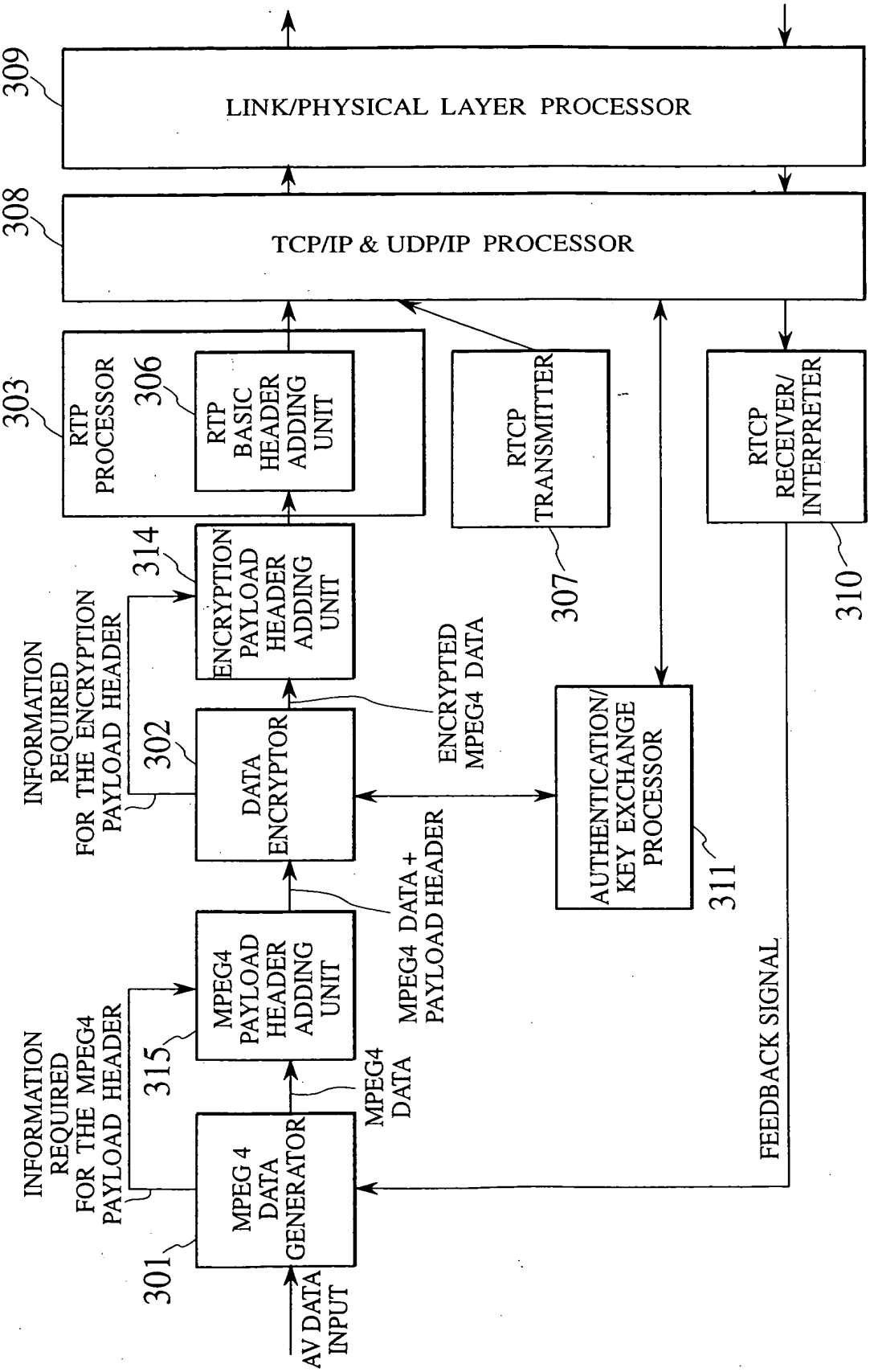


FIG. 19

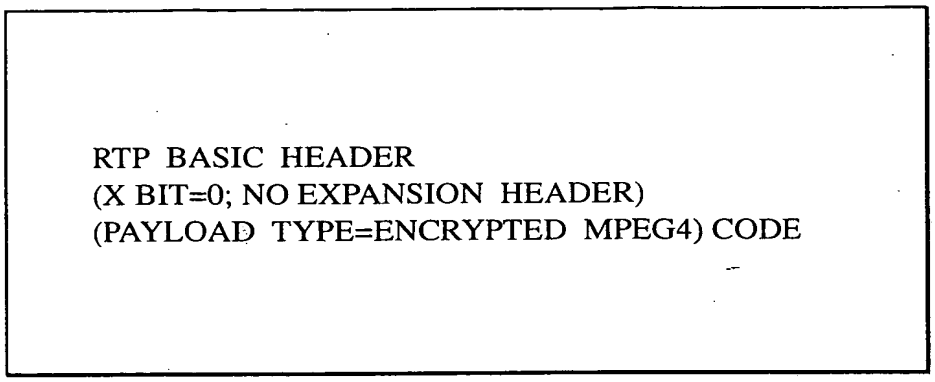

RTP BASIC HEADER
(X BIT=0; NO EXPANSION HEADER)
(PAYLOAD TYPE=ENCRYPTED MPEG4) CODE

FIG. 20

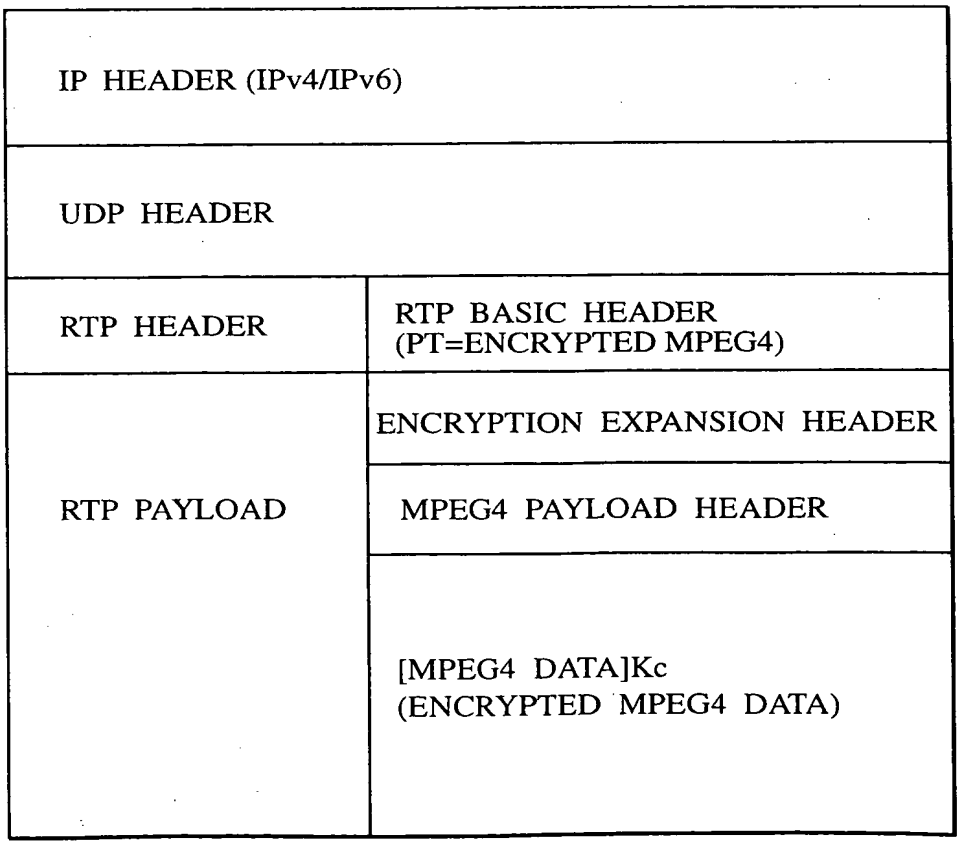

IP HEADER (IPv4/IPv6)
UDP HEADER
RTP HEADER
RTP BASIC HEADER
(PT=ENCRYPTED MPEG4)
RTP PAYLOAD
ENCRYPTION EXPANSION HEADER
MPEG4 PAYLOAD HEADER
[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)

FIG. 21

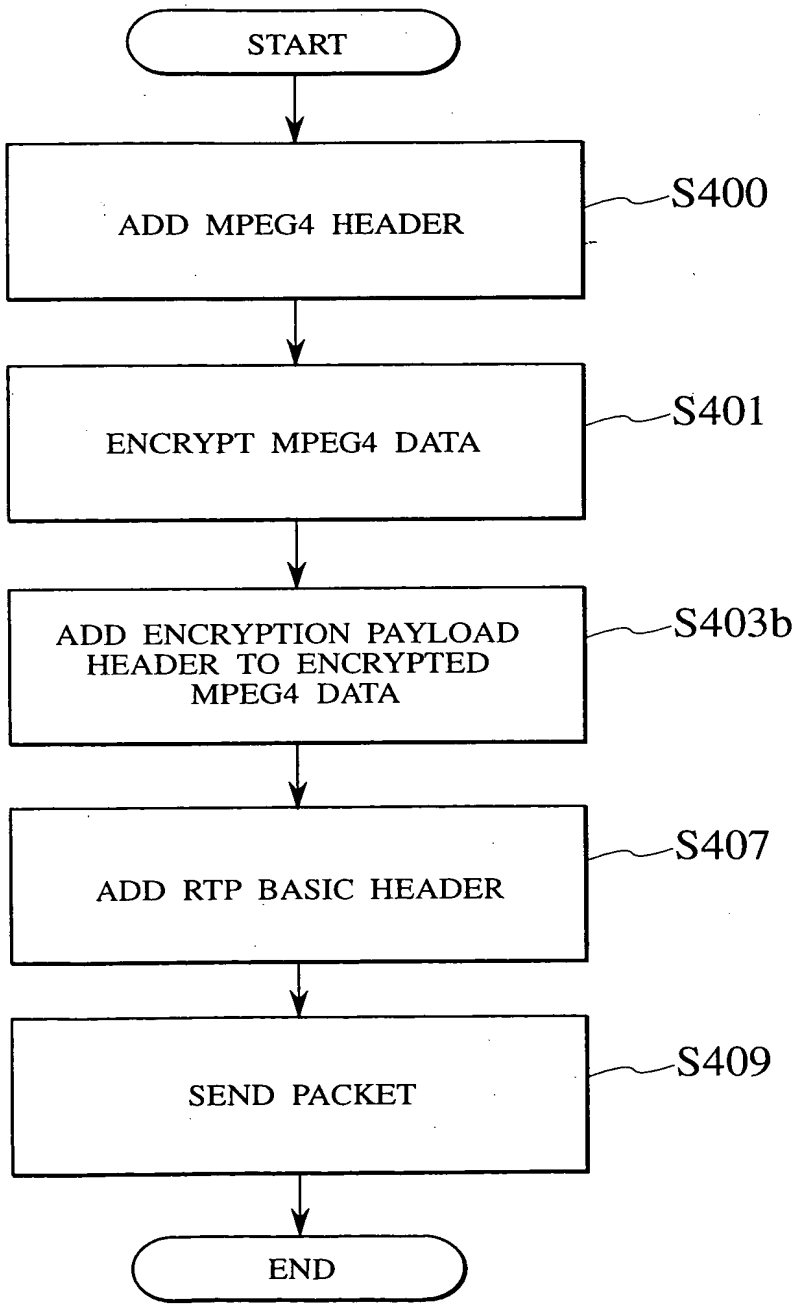

START
ADD MPEG4 HEADER
S400
ENCRYPT MPEG4 DATA
S401
ADD ENCRYPTION PAYLOAD HEADER TO ENCRYPTED MPEG4 DATA
S403b
ADD RTP BASIC HEADER
S407
SEND PACKET
S409
END

FIG. 22

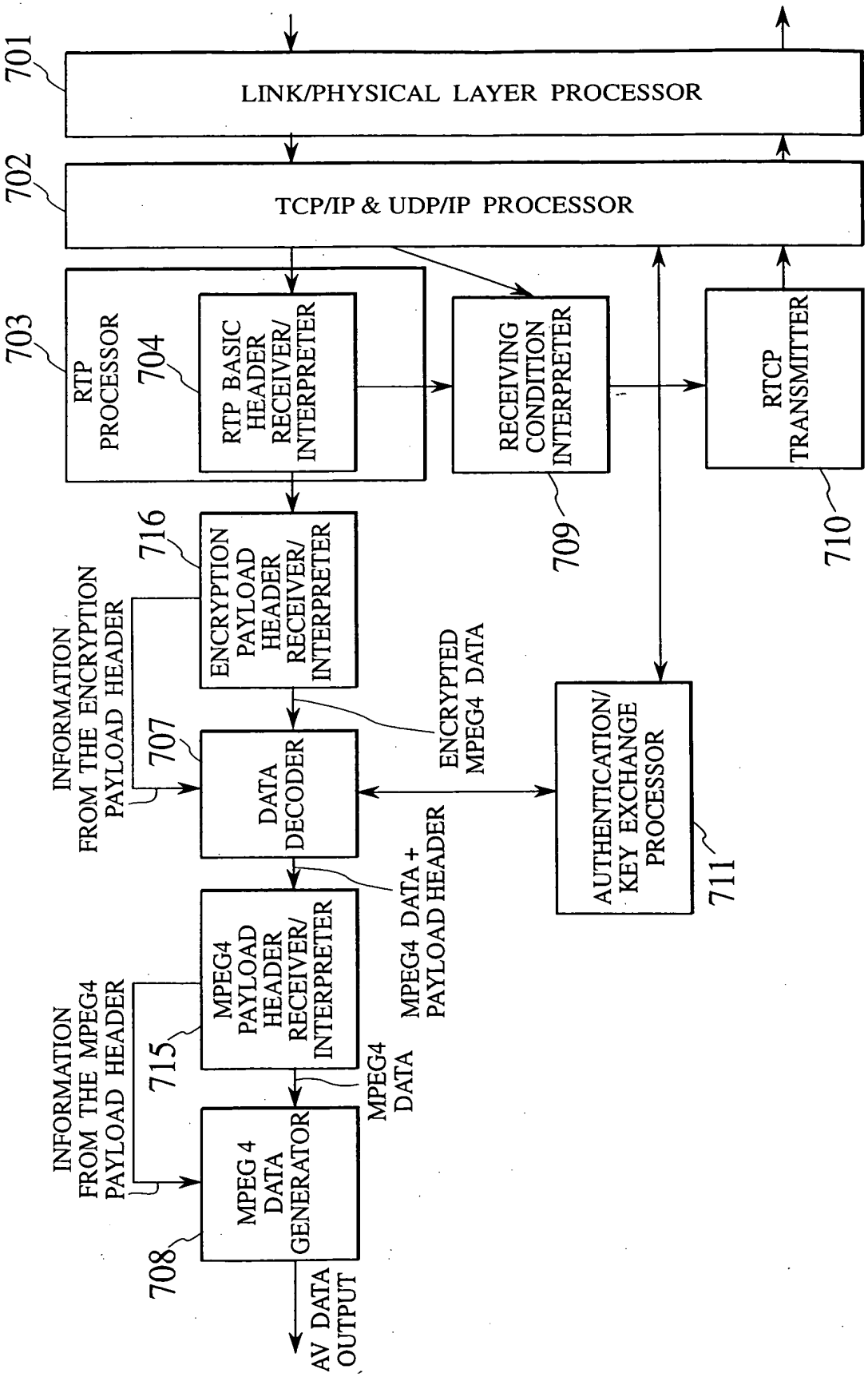

701
LINK/PHYSICAL LAYER PROCESSOR
702
TCP/IP & UDP/IP PROCESSOR
703
RTP PROCESSOR
704
RTP BASIC HEADER RECEIVER/ INTERPRETER
709
RECEIVING CONDITION INTERPRETER
710
RTCP TRANSMITTER
716
ENCRYPTION PAYLOAD HEADER RECEIVER/ INTERPRETER
INFORMATION FROM THE ENCRYPTION PAYLOAD HEADER
707
DATA DECODER
ENCRYPTED MPEG4 DATA
711
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
MPEG4 DATA + PAYLOAD HEADER
715
MPEG4 PAYLOAD HEADER RECEIVER/ INTERPRETER
INFORMATION FROM THE MPEG4 PAYLOAD HEADER
MPEG4 DATA
708
MPEG 4 DATA GENERATOR
AV DATA OUTPUT

FIG. 23

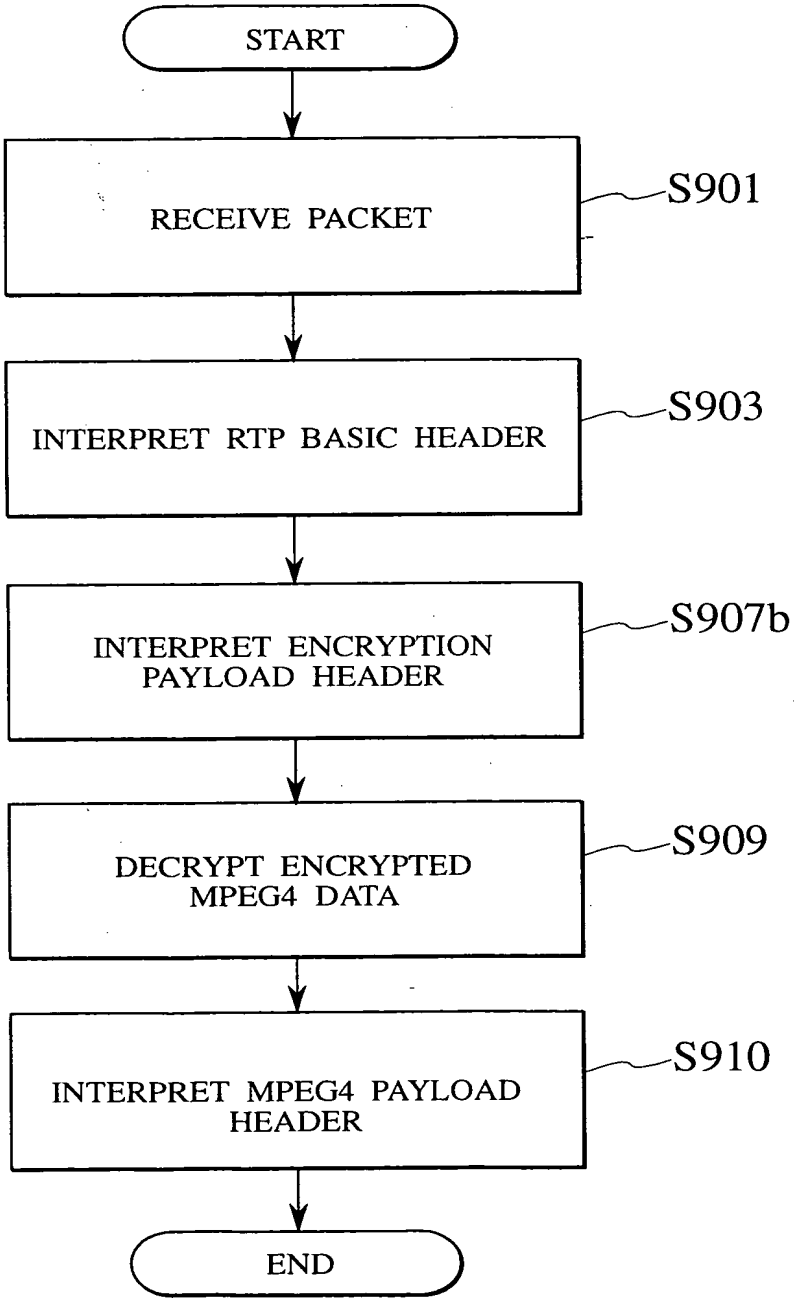

START
RECEIVE PACKET
S901
INTERPRET RTP BASIC HEADER
S903
INTERPRET ENCRYPTION PAYLOAD HEADER
S907b
DECRYPT ENCRYPTED MPEG4 DATA
S909
INTERPRET MPEG4 PAYLOAD HEADER
S910
END

FIG. 24

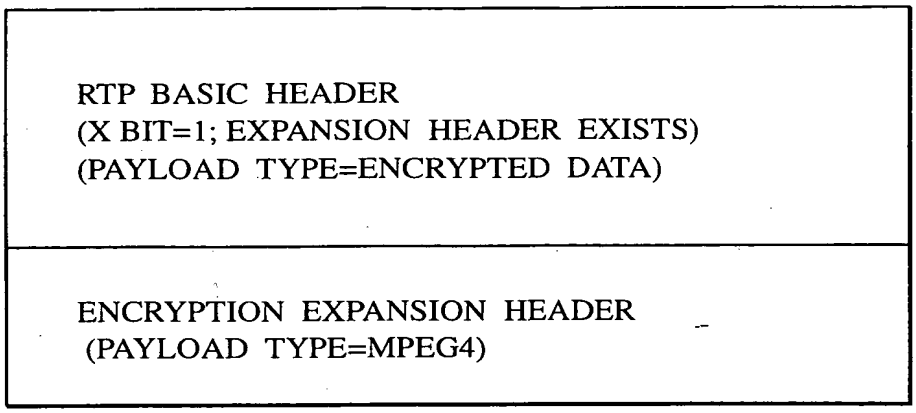

RTP BASIC HEADER
(X BIT=1; EXPANSION HEADER EXISTS)
(PAYLOAD TYPE=ENCRYPTED DATA)
ENCRYPTION EXPANSION HEADER
(PAYLOAD TYPE=MPEG4)

FIG. 25

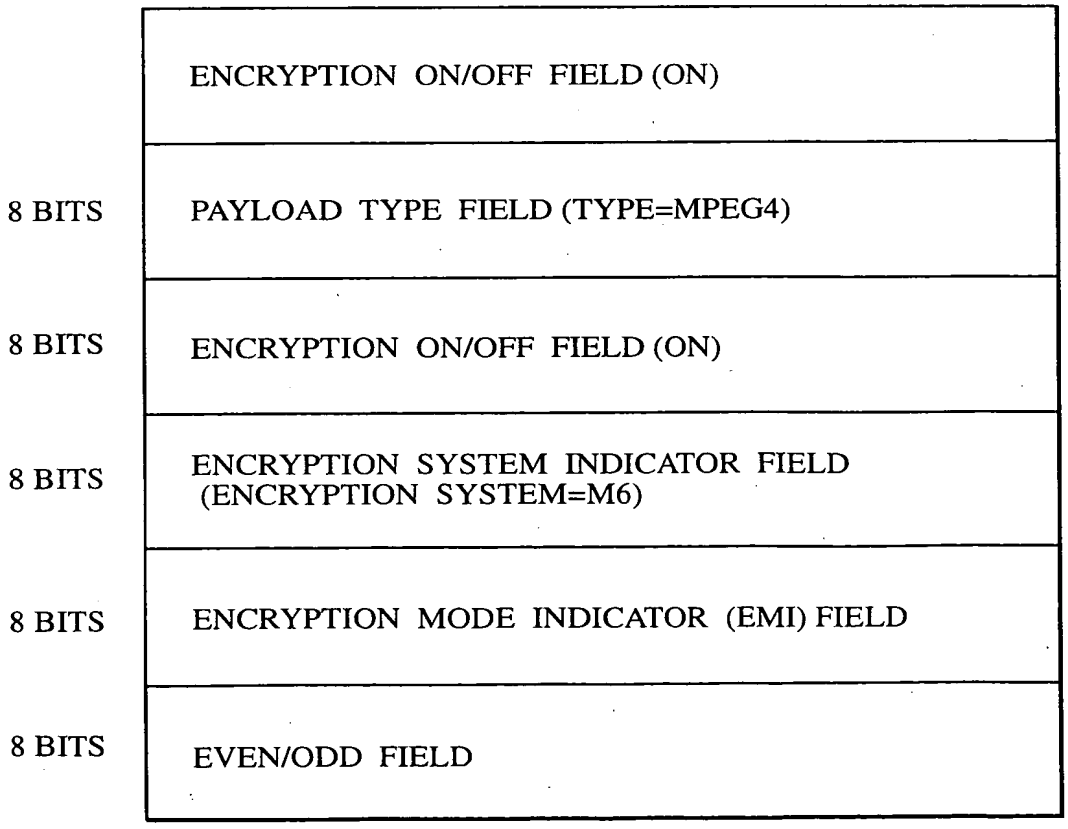

ENCRYPTION ON/OFF FIELD (ON)
8 BITS
PAYLOAD TYPE FIELD (TYPE=MPEG4)
8 BITS
ENCRYPTION ON/OFF FIELD (ON)
8 BITS
ENCRYPTION SYSTEM INDICATOR FIELD
(ENCRYPTION SYSTEM=M6)
8 BITS
ENCRYPTION MODE INDICATOR (EMI) FIELD
8 BITS
EVEN/ODD FIELD

FIG. 26

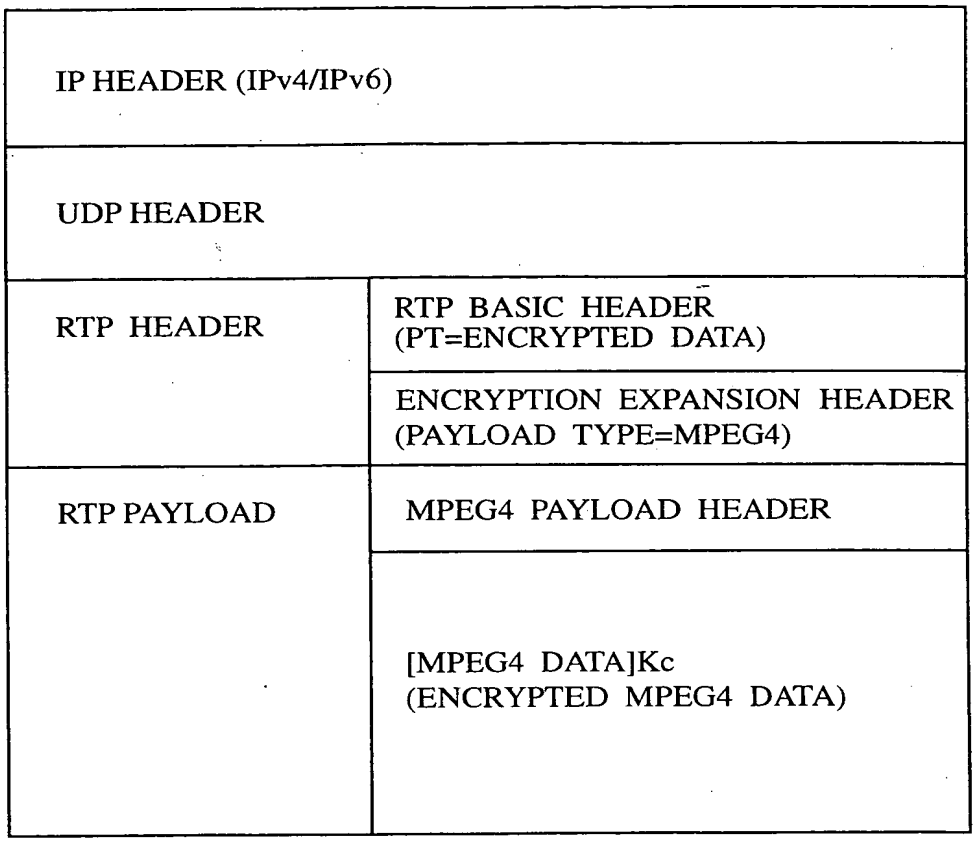

IP HEADER (IPv4/IPv6)
UDP HEADER
RTP HEADER
RTP BASIC HEADER
(PT=ENCRYPTED DATA)
ENCRYPTION EXPANSION HEADER
(PAYLOAD TYPE=MPEG4)
RTP PAYLOAD
MPEG4 PAYLOAD HEADER
[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)

FIG. 27

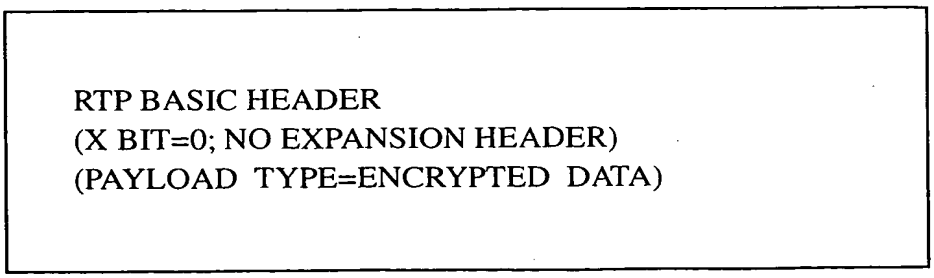

RTP BASIC HEADER
(X BIT=0; NO EXPANSION HEADER)
(PAYLOAD TYPE=ENCRYPTED DATA)

FIG. 28

<table>
<tr><td colspan="2">IP HEADER (IPv4/IPv6)</td></tr>
<tr><td colspan="2">UDP HEADER</td></tr>
<tr><td>RTP HEADER</td><td>RTP BASIC HEADER
(PT=ENCRYPTED DATA)</td></tr>
<tr><td rowspan="3">RTP PAYLOAD</td><td>ENCRYPTION EXPANSION HEADER
(PAYLOAD TYPE=MPEG4)</td></tr>
<tr><td>MPEG4 PAYLOAD HEADER</td></tr>
<tr><td>[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)</td></tr>
</table>

0002620 5450260

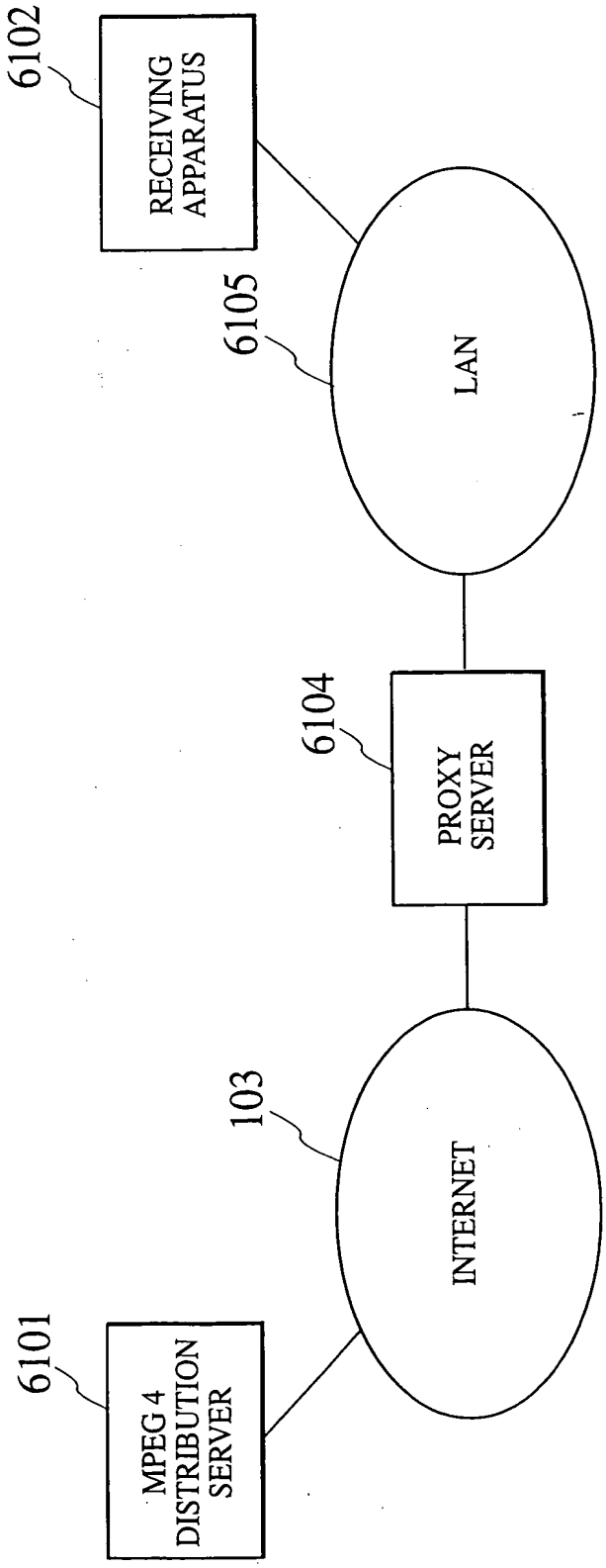

6102
RECEIVING APPARATUS
6105
LAN
6104
PROXY SERVER
103
INTERNET
6101
MPEG 4 DISTRIBUTION SERVER

FIG. 29

OBLON ET AL (703) 413-3000
DOCKET # M39-767 SHEET 24 OF 28

FIG. 30

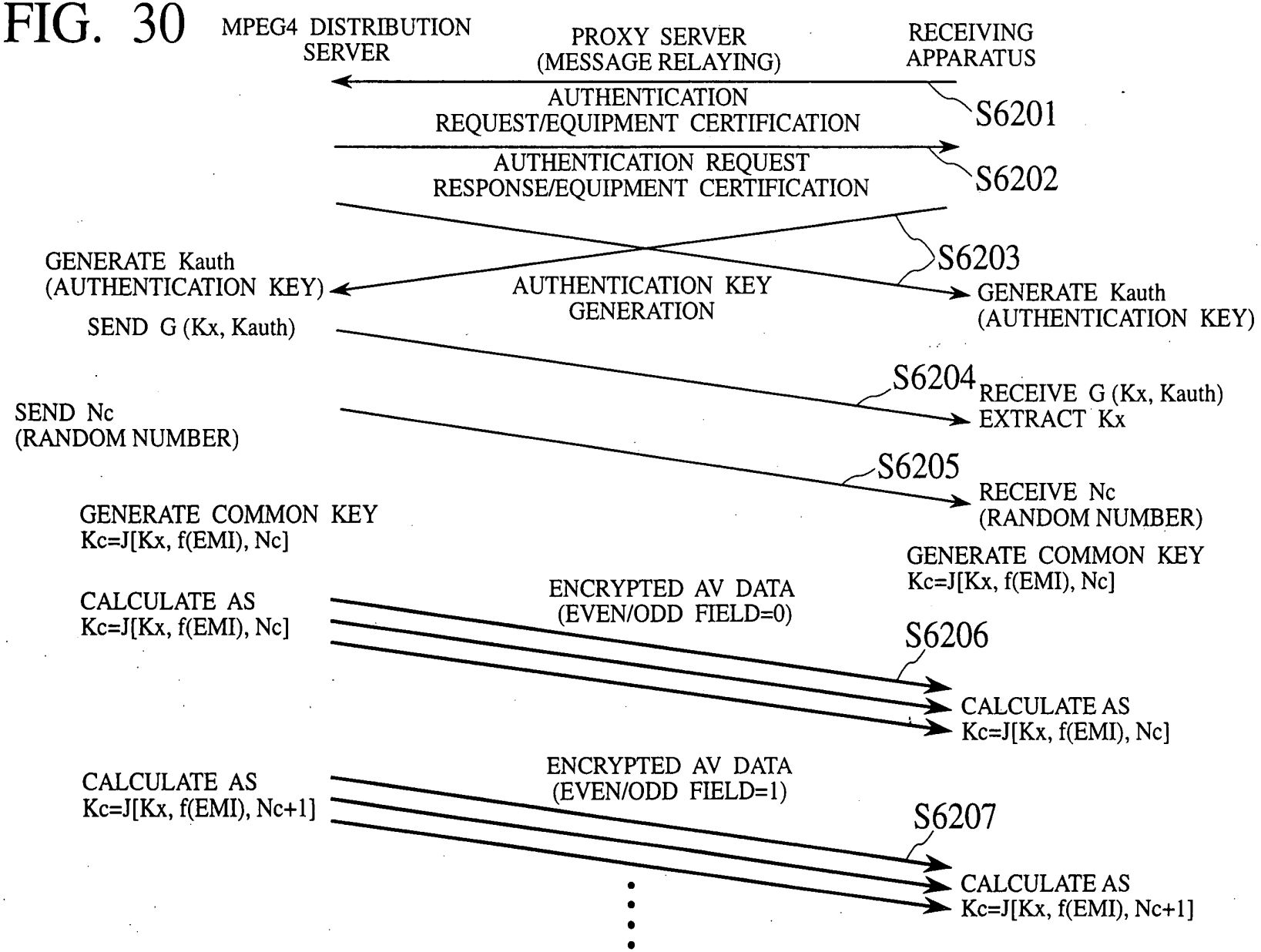


FIG. 31

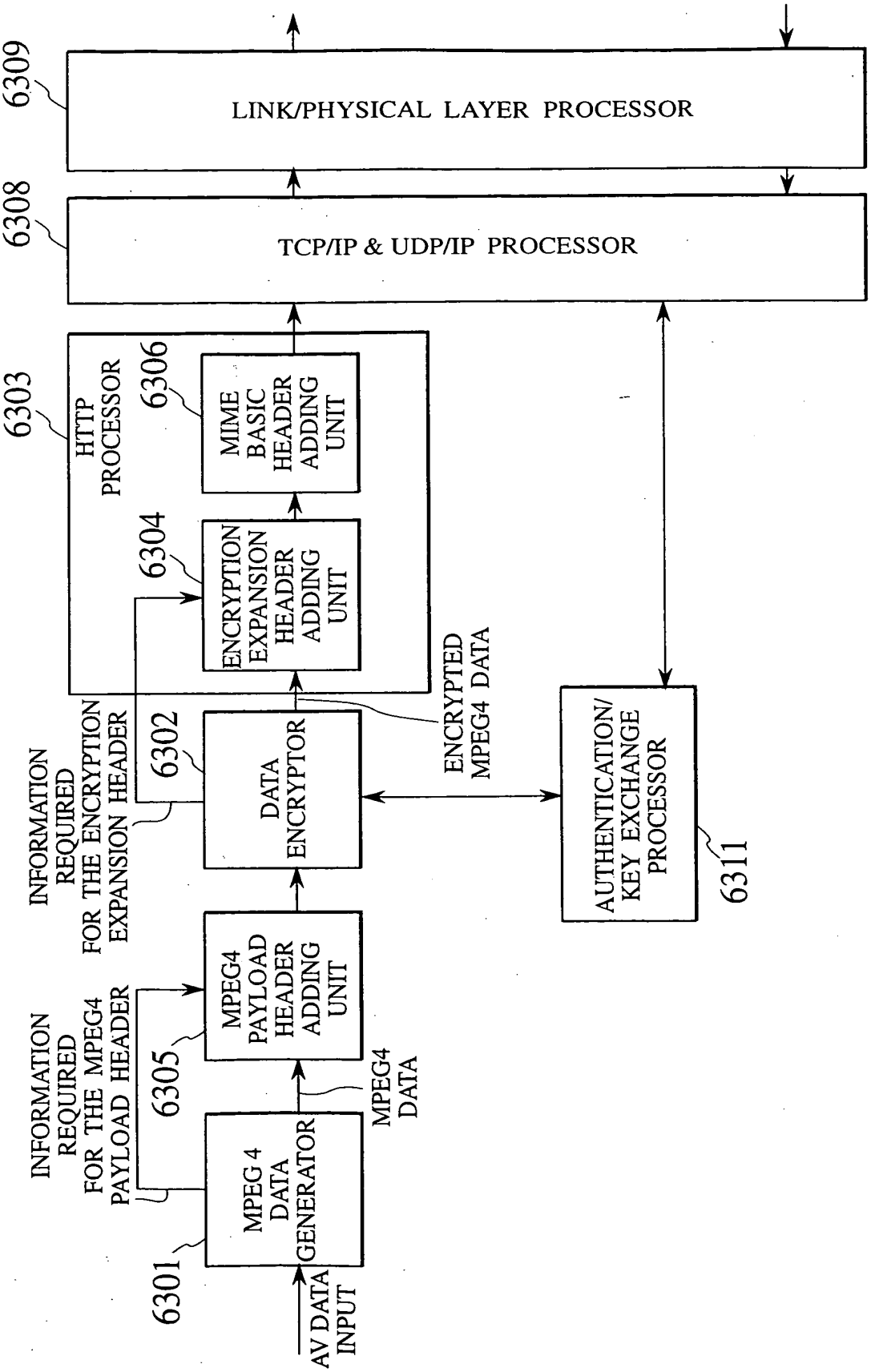

6309
LINK/PHYSICAL LAYER PROCESSOR
6308
TCP/IP & UDP/IP PROCESSOR
6303
HTTP PROCESSOR
6306
MIME BASIC HEADER ADDING UNIT
6304
ENCRYPTION EXPANSION HEADER ADDING UNIT
ENCRYPTED MPEG4 DATA
INFORMATION REQUIRED FOR THE ENCRYPTION EXPANSION HEADER
6302
DATA ENCRYPTOR
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
6311
INFORMATION REQUIRED FOR THE MPEG4 PAYLOAD HEADER
6305
MPEG4 PAYLOAD HEADER ADDING UNIT
MPEG4 DATA
6301
MPEG 4 DATA GENERATOR
AV DATA INPUT

FIG. 32

<table>
<tr><td colspan="2">IP HEADER (IPv4/IPv6)</td></tr>
<tr><td colspan="2">TCP HEADER</td></tr>
<tr><td colspan="2">MIME BASIC HEADER</td></tr>
<tr><td>Content-Type=
application/X-encription</td><td>ENCRYPTION EXPANSION HEADER</td></tr>
<tr><td rowspan="2">Content-Type=
application/X-MPEG4</td><td>MPEG4 PAYLOAD HEADER</td></tr>
<tr><td>[MPEG4 DATA]Kc
(ENCRYPTED MPEG4 DATA)</td></tr>
</table>

FIG. 33

<table>
<tr><td>MIME BASIC HEADER
MIME-Version:1.0
Message-ID:User1-1
Content-Type:Multipasrt/mixed
boundary=''-boundary1-''</td></tr>
<tr><td>ENCRYPTION EXPANSION HEADER
Content-Type=application/x-encription
ENCRYPTION SYSTEM INDICATOR FIELD (ENCRYPTION SYSTEM=M6)
ENCRYPTION ON/OFF FIELD (ON)
ENCRYPTION MODE INDICATOR (EMI) FIELD
EVEN/ODD FIELD</td></tr>
</table>

FIG. 34

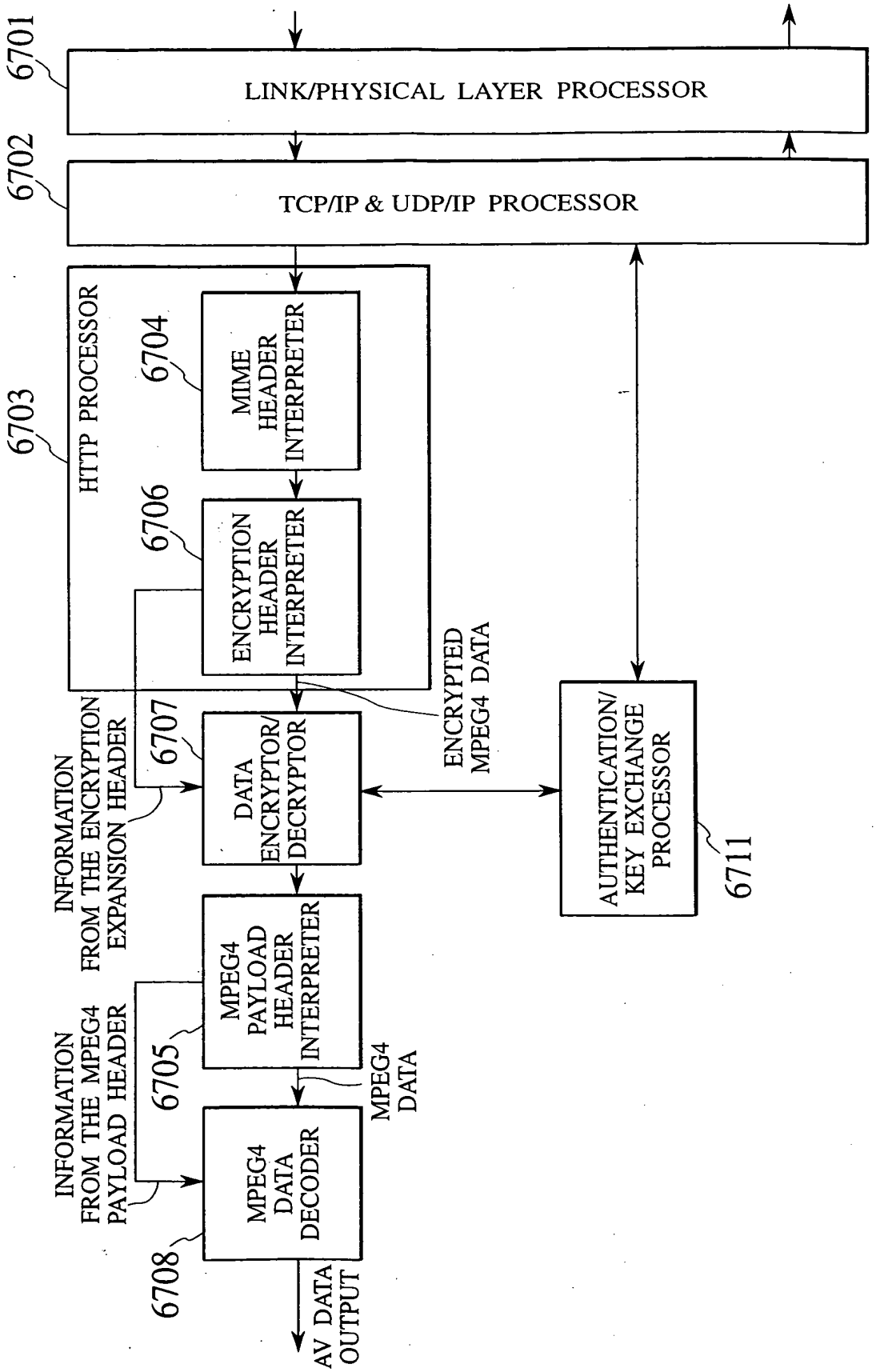
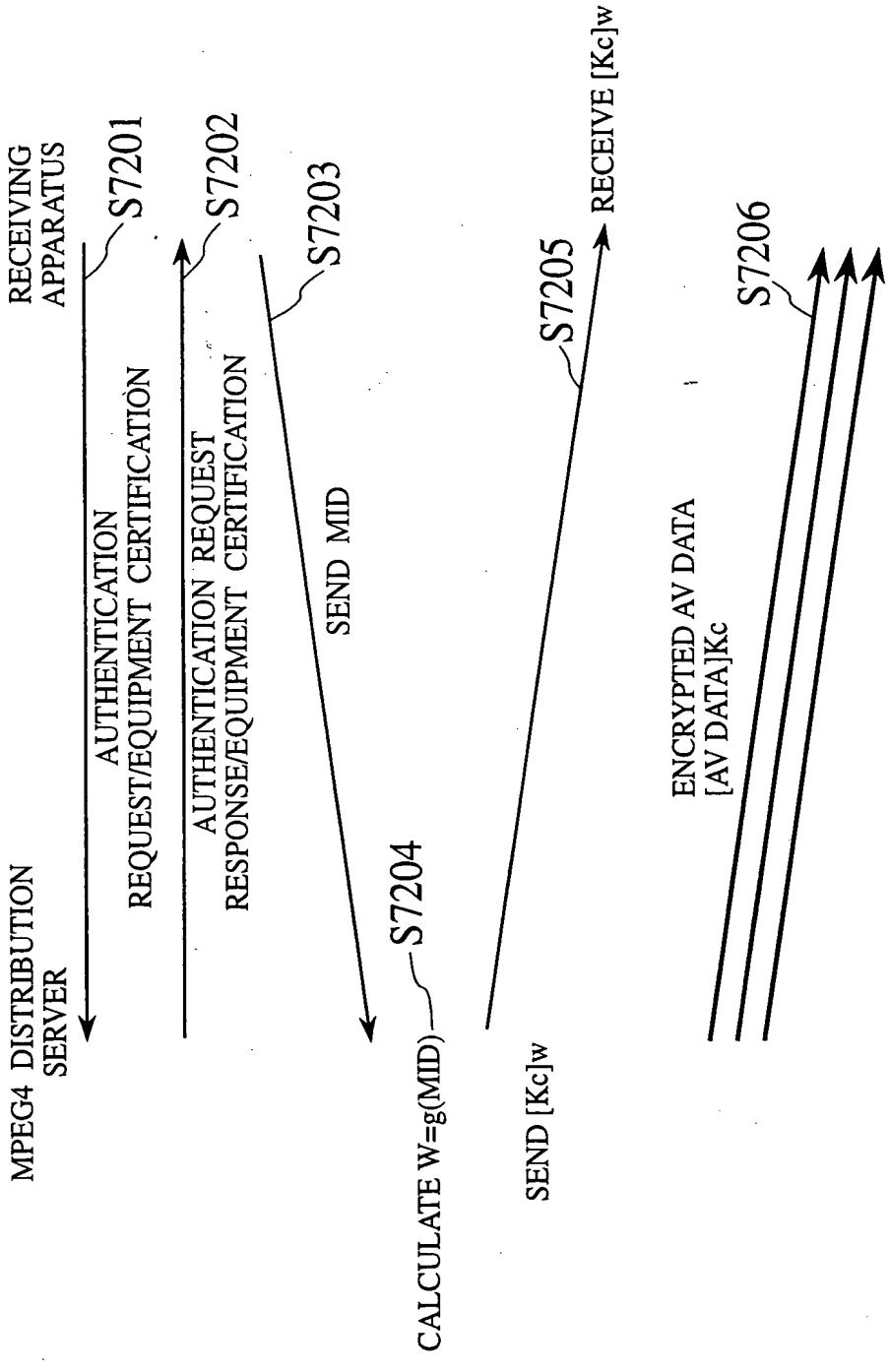

6701
LINK/PHYSICAL LAYER PROCESSOR
6702
TCP/IP & UDP/IP PROCESSOR
6703
HTTP PROCESSOR
6704
MIME HEADER INTERPRETER
6706
ENCRYPTION HEADER INTERPRETER
ENCRYPTED MPEG4 DATA
INFORMATION FROM THE ENCRYPTION EXPANSION HEADER
6707
DATA ENCRYPTOR/ DECRYPTOR
AUTHENTICATION/ KEY EXCHANGE PROCESSOR
6711
INFORMATION FROM THE MPEG4 PAYLOAD HEADER
6705
MPEG4 PAYLOAD HEADER INTERPRETER
MPEG4 DATA
6708
MPEG4 DATA DECODER
AV DATA OUTPUT

FIG. 35


RECEIVING APPARATUS
MPEG4 DISTRIBUTION SERVER
S7201
AUTHENTICATION REQUEST/EQUIPMENT CERTIFICATION
S7202
AUTHENTICATION REQUEST RESPONSE/EQUIPMENT CERTIFICATION
S7203
SEND MID
S7204
CALCULATE W=g(MID)
S7205
SEND [Kc]w
RECEIVE [Kc]w
S7206
ENCRYPTED AV DATA [AV DATA]Kc